

1/2

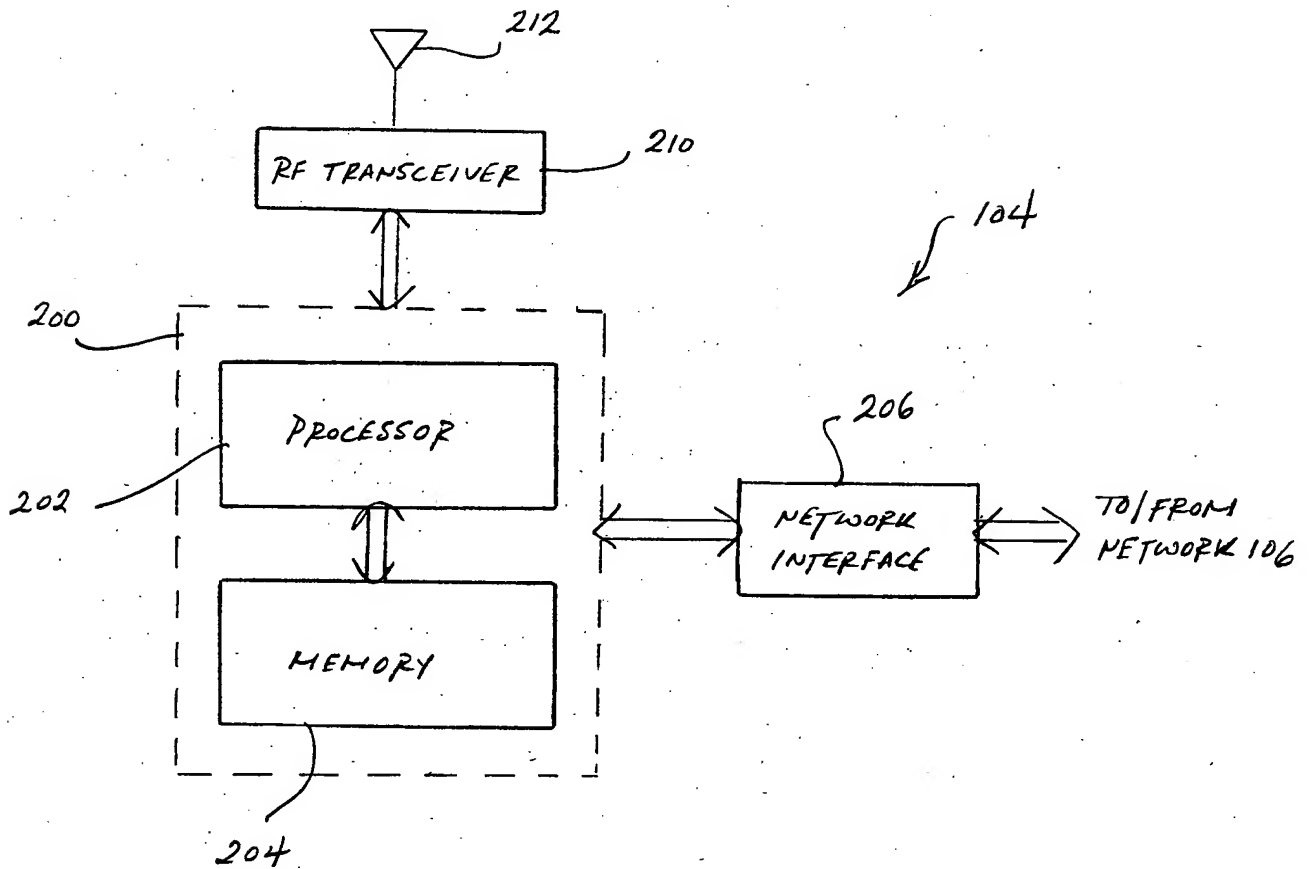
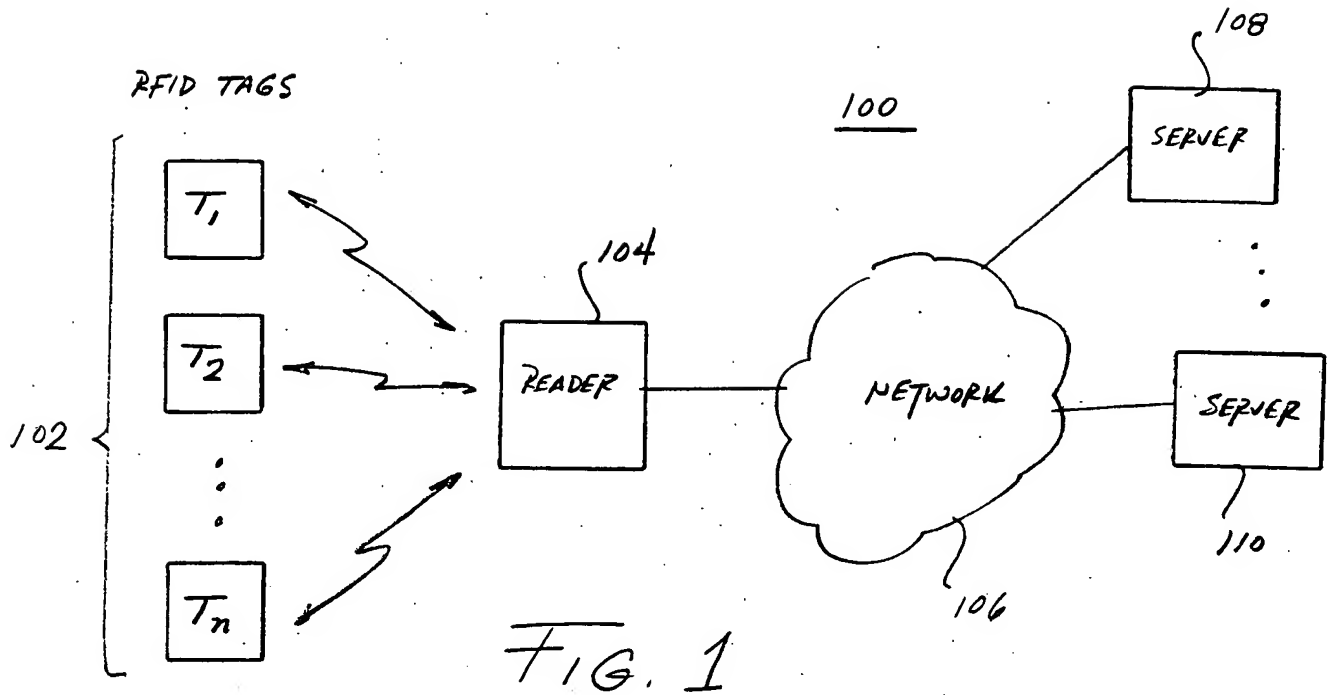


FIG. 2

Tag	Verifier
$d \leftarrow (c \bmod k) + 1$ $\alpha' \leftarrow \alpha_d$	if α' is valid α_i for some tag T_x then $\quad tag \leftarrow x$ $\quad \beta' \leftarrow \beta_i$ $\quad \gamma \leftarrow \gamma_i$ \quad mark α_i as invalid for T_x else \quad output("reject") and abort
if $\beta' \neq \beta_d$ then \quad output("reject") and abort $\gamma' \leftarrow \gamma_d$	$\beta' \leftarrow$
$\{\text{update}(\Delta_\kappa, \bar{\Delta}_\kappa)\}_{\kappa \in ABC}$ $\{\kappa \leftarrow \text{pad}(\kappa, \Delta_\kappa)\}_{\kappa \in ABC}$ $c \leftarrow c + 1$	if $\gamma' \neq \gamma$ or $\gamma' = \perp$ then \quad output("reject") and abort $\quad \bar{\Delta}_{ABC} \in_R \{0, 1\}^{3km}$
	$\bar{\Delta}_{ABC} \leftarrow$
	output(tag, "accept") $\{\text{update}(\Delta_\kappa, \bar{\Delta}_\kappa)\}_{\kappa \in ABC}$ $\{\kappa \leftarrow \text{pad}(\kappa, \Delta_\kappa)\}_{\kappa \in ABC}$

FIG. 3